What is claimed is:

1. A method for restoring a computer system modified by malicious code, comprising:

scanning the computer system for the malicious code;

identifying the malicious code;

retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and

executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

2. The method of claim 1, wherein the step of executing the at least one command includes one of reading, writing, and deleting data.

3. The method of claim 1, wherein the step of executing the at least one command includes at least one of renaming and deleting a file.

4. The method of claim 1, wherein the malicious code modifies at least one file and said method comprises:

reading from the modified file, a name of a second file; and

modifying the second file.

5. The method of claim 1, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.

6. A storage medium including computer executable code for restoring a computer system modified by malicious code, comprising:

code for scanning the computer system for the malicious code;

code for identifying the malicious code;

code for retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and

code for executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

7. The storage medium of claim 6, wherein the code for executing the at least one command includes code for performing at least one one of reading, writing, and deleting data.

8. The storage medium of claim 6, wherein the code for executing the at least one command includes code for performing at least one of renaming and deleting a file.

9. The storage medium of claim 6, wherein the malicious code modifies at least one file, said storage medium further comprising:

code for reading from the modified file, a name of a second file; and

code for modifying the second file.

10. The storage medium of claim 6, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.

11. A computer data signal embodied in a transmission medium and including computer executable instructions for restoring a computer system modified by malicious code, comprising:

a data signal portion for scanning the computer system for the malicious code;

a data signal portion for identifying the malicious code;

a data signal portion for retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and

a data signal portion for executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

12. The computer data signal of claim 11, wherein the data signal portion for executing the at least one command performs at least one of reading, writing, and deleting data.

13. The computer data signal of claim 11, wherein the data signal portion for executing the at least one command performs at least one of renaming and deleting a file.

14. The computer data signal of claim 11, wherein the malicious code modifies at least one file, said computer data signal further comprising:

a data signal portion for reading from the modified file, a name of a second file; and

a data signal portion for modifying the second file.

15. The computer data signal of claim 11, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.

16. A programmed computer system including a program for restoring a computer system modified by malicious code, comprising:

means for scanning the computer system for the malicious code;

means for identifying the malicious code;

means for retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and

means for executing the at least one command to restore the computer system to substantially the state as it existed prior to modification by the malicious code.

17. The programmed computer system of claim 16, wherein the means for executing the at least one command includes means for performing at least one of reading, writing, and deleting data.

18. The programmed computer system of claim 16, wherein the means for executing the at least one command includes means for performing at least one of renaming and deleting a file.

19. The programmed computer system of claim 16, wherein the malicious code modifies at least one file and said system further comprises:

means for reading from the modified file, a name of a second file; and

means for modifying the second file.

20. The programmed computer system of claim 16, wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code.